A Framework for SDN Forensic Readiness and Cybersecurity Incident Response

1st María B. Jiménez
(PhD Student)
Department of Telematics Engineering
Universidad Politécnica de Madrid
Madrid, Spain
mb.jimenez@alumnos.upm.es

2nd David Fernández
(Supervisor)
Department of Telematics Engineering
Universidad Politécnica de Madrid
Madrid, Spain
david.fernandez@upm.es

2022 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN) | 978-1-6654-7334-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/NFV-SDN56302.2022.9974648

***Abstract*—SDN represents a significant advance for the telecom world, since the decoupling of the control and data planes offers numerous advantages in terms of management dynamism and programmability, mainly due to its software-based centralized control. Unfortunately, these features can be exploited by malicious entities, who take advantage of the centralized control to extend the scope and consequences of their attacks. When this happens, both the legal and network technical fields are concerned with gathering information that will lead them to the root cause of the problem. Although forensics and incident response processes share their interest in the event information, both operate in isolation due to the conceptual and pragmatic challenges of integrating them into SDN environments, which impacts on the resources and time required for information analysis. Given these limitations, the current work focuses on proposing a framework for SDNs that combines the above approaches to optimize the resources to deliver evidence, incorporate incident response activation mechanisms, and generate assumptions about the possible origin of the security problem.**

***Index Terms*—SDN Forensics, Evidence, Digital Forensic, SDN Incident Response, SDN Security, SDN Framework**

I. Introduction

So far this year, cyberattacks have increased by 42% in comparison to the previous year [1]. Given that the SDN paradigm has become more prevalent in the deployment of telecommunication services, it cannot be dismissed that many of these attacks have targeted these sorts of networks, especially considering the vulnerabilities of its architecture [2].

When a cybersecurity incident occurs in an organization or company, it is necessary to find the origin of the problem, for which security event information is used. This essential information is gathered with the support of proper forensic readiness.

Forensic science has seen an upsurge in recent years since through its interaction with other disciplines, it has been able to address operational issues, recover data, identify policy and audit violations, etc. [3]. In this sense, in a cybercrime scene, the security event information enables the creation of an evidence map that can be used in a legal proceeding.

From a technical perspective, it has been observed that forensic processes strengthen incident response lifecycle processes, as event information can be used to reconstruct attack scenarios and thus improve security policies.

Since forensic and incident response processes have a common interest in security event information, it would be ideal to manage them simultaneously, in order to optimize the use of resources and reduce the time spent on data analysis. Unfortunately, there are several challenges related to implementing the forensic processes within an SDN context, and little is said about its association with other processes.

Facing those challenges, this paper focuses on defining a framework that incorporates forensic and incident response lifecycle processes in SDN environments. In this way, it outlines the strategies used to optimize resources that allow: providing evidence, triggering early responses to security incidents, and making assumptions about the origin of the security problem.

It is worth noting that the scope of this article with respect to the delivery of evidence does not contemplate a particular jurisdictional understanding but a general legal vision.

A. Problem Statement and Challenges

According to a study formulated by Gartner, despite network cybersecurity incidents of a company or organization are considered a corporate risk, internally, these problems must be dealt with by the IT department [4]. In this sense, this department should respond to a security incident and simultaneously activate operational tasks for gathering evidence.

Unfortunately, when a network security incident occurs, the IT department focuses all its efforts on containing it. And due to the endured stress, the forensic process is postponed or even omitted. These gaps between incident response and forensic process management makes that each area involved, legal or technical, acts spontaneously and improvised to gather information about what happened.

By not adequately linking the forensic and incident response processes, the interested areas try to obtain as many data

This work was supported by the Ecuadorian funding institute SENESCYT-Secretaría de Educación Superior, Ciencia, Tecnología e Innovación, under the Ph.D. Grant CZ02-000486-2019. Additionally, this work was supported in part by the Spanish Ministry of Science and Innovation in the context of the ECTICS project (PID2019-105257RB-C21) and by the Spanish Ministry of Science, Innovation and Universities in the context of the Go2Edge project (RED2018-102585-T).

as they can, from different sources of information, with specifications and time frames adjusted to their visions. These uncoordinated actions are counterproductive and time consuming, affecting the quality and the effectiveness of the process of finding the origin of the problem; thus, generating serious repercussions on the company's reputation and the quality of the delivered services.

Moreover, several technical challenges arise regarding the implementation of forensic processes in SDNs, namely: the security of the evidence, the network performance during forensic processes, the possible spoofing of evidence sources, the log synchronization when there are several SDN controllers, the cost-benefit of forensic readiness, the lack of forensic expertise and the implementation policies in SDN environments, and the performance; especially in processing and storage [3], [5]. Regarding the implementation of incident response processes, the main concerns are the treatment of individual events, the time spent on information analysis and the risk of handling false positives [6].

Considering the above challenges and issues, this paper introduces a framework for integrating forensic and incident response processes in an SDN context. This framework offers a solution to the information management conflict and resource usage when a security event occurs. Through this framework, the main forensic and incident response actions in an SDN environment are described such as supplying evidence, triggering early response mechanisms to cybersecurity incidents, and providing assumptions regarding the origin of the security problem.

The rest of the paper is structured as follows. Section II presents forensic and incident response background, describing the main related works and stating the contributions of this research. Section III describes the current state of the research including its main challenges, the development of the proposed framework and some details of the implementation of a proof-of-concept prototype.

II. Background, Related Literature and Contributions

A. Forensics and Incident Response Terms

Digital forensics is a broad and relevant part of forensic sciences that focuses on gathering digital evidence from different sources of information such as hardware, software, or network data. Digital forensics has a specialized area called Network forensics for the study and collection of digital evidence from the network and its moving traffic. This forensic sub-branch is leveraged on traffic monitoring and intrusion detection to identify and solve security vulnerabilities in the network, and improve the allocation of resources during a cybersecurity incident [7], [8].

A digital forensic process can be either live or post-mortem. The former, also known as proactive/dynamic forensic, is oriented towards volatile data acquisition, fetching information while the source is active. On the other hand, the post-mortem, or so-called reactive/static forensic, analyses stored data once the information sources are inactive [9].

Digital forensic readiness is a proactive measure to capture information from a potential security event. In this way, it tries to maximize the technological capabilities of an environment for activities registration and evidence collection, minimizing the impact on resources during the digital forensic process [10].

To conduct a digital forensic process, ISO/IEC 27042 [11] defines the following phases: collection, examination, analysis, and reporting. The essential information obtained from a forensic process can be used in both legal and technical fields [10]. For data to be used as a probative resource in a legal proceeding, it must be: relevant, authentic, accurate, complete, consistent, reliable, and transparent [12].

From a technical perspective, the information obtained from forensic processes supports the lifecycle of incident response within an organization. Through data event analysis, it is possible to remediate and recover the affected technological resources. Similarly, once the evidence is assembled, the adoption of security policies can be improved to provide shorter response times in technical solutions. NIST SP 800-61r2 [13] defines the phases of an incident lifecycle as: preparation, detection and analysis, containment, eradication and recovery, and post-incident activity.

B. Related Literature and Contributions

As explained above, forensic science is a booming branch. As far as SDN is concerned, it is still in the development phase. In this light, some emerging research have been paving the way to improve its implementation. For instance, the authors of [14] propose a forensic conceptual framework for carrying out an evidence delivery process, including a description of its main modules, objectives, and design requirements. The authors note that data extraction and fusion are being investigated, and as future work they plan to develop a software prototype.

Observing the challenges of evidence reliability, the authors of [15] propose a dynamic forensic approach for environments working with SDNs. They point out that the forensic process initialization employing a trigger mechanism improves accuracy and evidence collection. As an extension to the latter framework, Lagrasse et al. [16] propose a forensic framework with an IDS-trigger-based collection mechanism, using Snort IDS policies to reduce evidence storage requirements. Unfortunately, the use of this IDS over the deployed infrastructure causes scalability issues.

To ensure the chain of custody of the collected data, the authors of [17] propose a forensic architecture for SDN-IoT environments using distributed ledger technology. Similarly, in [18], the authors present a blockchain-based mechanism to secure logs of some SDN elements.

On the other hand, some authors propose forensic solutions oriented to the technical approach, although their proposals do not consider the delivery of evidence for its use in a process of law. Thus, in [19] the authors present a proposal to provide diagnostics for security solutions leveraged on the preprocessing of control plane event-oriented execution traces and data plane

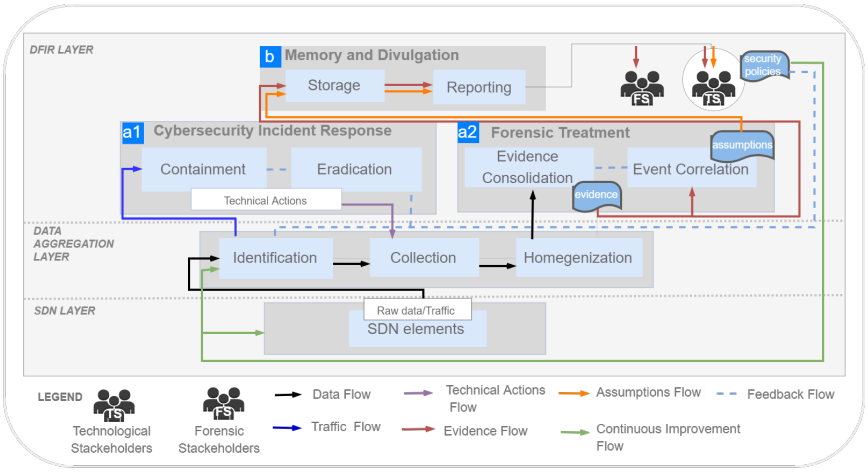

Fig. 1. High-level description and workflow of proposed SDN Forensic Readiness and Cybersecurity Incident Response Framework.

state transition graphs. In [20] the authors present evidence-based technical processes for resolving security incidents such as DoS and topology poisoning.

In this line, some authors focus on data collection and reduction. For instance, in [21] the authors propose a framework for forensic investigation in Openflow-based SDN platforms. In this proposal, the data is fetched through packet captures of the southbound interface and memory images of the SDN switches. Whereas the data reduction process is carried out using an ontological method.

Likewise, some proposals use SDN architecture components to propose forensic solutions in areas namely IoT or Cloud Computing [22], [23]. However, these solutions do not cover SDN environments' legal and technical needs.

According to the state-of-the-art revision, it is observed that forensic and incident response processes have not been addressed holistically. Thus, solutions are delivered either for legal or technical purposes. To perform the forensic preparation, some authors limit themselves to taking the controller logs as the single data source, discarding other information locations.

In addition, most proposals focus exclusively on the acquisition and retention of data (evidence) and omit the crucial examination process, which can result in the delivery of redundant information, increasing analysis times.

To the best of our knowledge, this is the first work that incorporates the incident response lifecycle into the digital forensic process for SDNs. Apart from presenting a novel framework that manages these two approaches, this proposal:

- considers the use of multiple sources of information to provide more reliable evidence.
- uses trigger mechanisms for data collection to optimize performance in terms of storage and processing.
- proposes initialization mechanisms for early incident response to prevent further damage to the SDNs.
- maintains proper chain of custody (CoC) management.
- enables assumptions generation based on evidence to take corrective actions in the SDN environment.
- provides immutable storage of evidence and assumptions regarding the possible security incident's origin.

III. Current Status

Once the state of the art is reviewed, this section focuses on outlining the research work status on the proposed contributions.

A. Research Challenges

This section explains the main conceptual and pragmatic challenges of the research. At the same time, the strategies or mechanisms to address the challenges identified are described.

Considering that incident response processes rely on the information provided by a forensic process and that the link between these two concepts has not yet been merged in SDN environments, the first challenge of this proposal is to fuse these two concepts for efficient resource management. To this end, a framework has been defined, which is shown in Figure 1 and explained in more depth below.

Besides, other challenges will be addressed such as the reliability of the information, the amount of information to be processed and stored, the security of evidence, the integrity of the CoC, and the handling of false positives. To address them, this proposal includes: the management of multiple sources of information, the use of mechanisms for triggering incident response and data collection only upon detection of SDN element state changes or unusual traffic, the reduction of data dimensionality, and the use of distributed ledger technology. The details will be explained in the framework description.

B. Proposed SDN Forensic Readiness and Cybersecurity Incident Response Framework

The description and workflow of the proposed framework for SDN forensic readiness and cybersecurity incident response is depicted in Figure 1. This proposal dynamically optimizes some phases of the forensic and incident response processes proposed by [11] and [13], respectively. Its goal is to properly manage the data of SDN elements to provide

relevant, valid, and consistent evidence for a legal investigation process while using the available information to find solutions to cybersecurity issues in SDNs, through the incident response lifecycle. The description of each layer of the proposed framework is explained below.

SDN Layer

Since the logs, whether from the controller or security tools such as IDS, firewalls, etc., can be ambiguous and negate their usefulness in a technical or legal setting, information from corroborative sources is used to build more reliable assumptions [24]. In this sense, this framework incorporates additional SDN information sources such as communication interfaces, applications, and the data plane; since when any action occurs in the network, valuable information is generated that can be used as a means of corroboration to consolidate evidence and create robust event scenarios. Given this, SDN elements data will be retrieved from this layer to consolidate the evidence.

Although each SDN element provides specific types of data (e.g., logs, flow information, information received from APIs, etc.), in this document they will be referred to as raw data. The raw data provided by the SDN layer is classified as control raw data or traffic raw data. The control raw data includes the management actions of the SDN environment, such as controller login sessions, topology and application status change, etc., whilst the raw traffic data refers to the details of the SDNs flows.

On the other side, as part of the incident response process, containment actions will be executed on the SDN elements as soon as an unusual behavior is detected in the SDN or remedial actions when new security policies are applied.

Data Aggregation Layer

As mentioned above, one of the main concerns of implementing a forensic process is the storage capacity, and one of the main concerns of incident response is the time spent analysing information, especially from various sources. In this sense, this approach contemplates a collection mechanism associated with a security event. To this end, it is proposed to perform two relevant actions: identification and dimensionality reduction.

The identification action, detects unusual behavior in network traffic and changes in the state of the SDN elements.

The state-change detection of SDN elements is useful for finding clues that lead to a dynamic chain of events, for instance, in a cross-app poisoning attack [25]. Whilst, in the unusual behavior detection in SDN traffic, patterns are searched for that deviate from the expected traffic behavior. In this way, a comparison is performed between the incoming traffic and the original security rules defined by the technical stakeholders as part of the business requirements. Since there may be a margin of error in detecting unusual traffic behavior in terms of false positives; this framework considers forwards the traffic coming from the SDN layer to the cybersecurity incident response sub-layer to be re-evaluated. Once a change of state or unusual traffic behavior has been detected, the raw data collection begins through a secure channel.

Subsequently, to reduce the number of entries to be processed, a mechanism called feature engineering or feature selection is used, extracting only the relevant and representative fields from each record.

Thus, if a record A contains n entries, but of those entries only x are linked to an event; the useful record will not be $A{=}n$, but instead $A{=}n'$ [26]. After the acquisition, the collected data is standardized to facilitate its processing.

Digital Forensic and Incident Response Layer (DFIR)

The aim of this layer is to handle forensic and incident response processes simultaneously. Task processing is defined by each of its sub-layers, as shown described below:

a1. Cybersecurity Incident Response Sub-layer: activates the technical mechanisms to contain and eradicate the security incident. In a containment phase, temporary actions, like rerouting network traffic, are implemented as a remedial measure.

Then, in an eradication phase, final solutions are developed based on new security policies to eliminate the cause of the security incident. Eradication actions are associated with the data aggregation or SDN layers. In the SDN layer, changes can be made to the forwarding actions of SDN switches. In the data aggregation layer, new filtering parameters are defined.

Each time an action is taken against an incident, this layer is responsible for sending information about the used techniques or commands, which feeds into the evidence consolidation process. In this sense, it is possible to know exactly what operations were carried out, which techniques were used, and how much time elapsed in carrying them out. This information enriches the forensic process and serves as a reference for future cybersecurity incidents.

a2. Forensic Treatment Sub-layer: consolidates raw data to provide evidence once an event has occurred. It is also responsible for inferring the possible causes of a security problem in the network.

Consolidation is based on chronological grouping and consistency checking of collected and standardized data. Chronological consolidation groups data from different information sources according to a timeline, whereas consistency checks duplicate records or missing information. At this point, it is possible to use the data as evidence. The evidence is passed to the memory and divulgation sub-layer to meet legal requirements.

A correlation of events is created to fulfill the technical requirements. In this manner, this sub-layer takes all the individual events and relates them to depict a security problem. Subsequently, the possible assumptions are passed on to the upper sub-layer so stakeholders adopt or discard new security policies.

b. Memory and Divulgation Sub-layer: strengthens the security of the CoC, avoiding manipulations on the evidence and on the assumptions of the cybersecurity incident origin. To achieve this goal, this framework relies on the use of distributed ledger technology, which provides immutability to information and preserves the records of transactions that take place during storage. In this way, the principles of confidentiality, integrity and availability are met for the admission of evidence in legal proceedings. Starting from the information stored in this sub-layer, reports are generated for each stakeholder according to their assigned roles.

C. Implementation, Early Indicative Results and Open Questions

This section introduces the scenario in which the aforementioned contributions are validated. This test aims to assess the effectiveness of filtering, data reduction, and therefore the optimization of storage resources for the provision of evidence. A virtual environment has been deployed where an ICMP flood attack against the controller, changes in the applications status, and changes in the topology of the SDN are simulated. For this purpose, the controller logs, the Openflow channel information, and the responses from the controllers' REST API are used. The test environment comprises three virtual machines (VM). In the first VM, a custom containerized ONOS instance was deployed. The image contains a script written in Bash to extract the controller logs. The second VM implements the topology, comprised of an ONOS controller, five OVS switches v1.3 in a star distribution, and 20 hosts. To simulate normal traffic and an ICMP saturation of the controller a Python script was developed. On a third host, the evidence is filtered, collected, standardized, and consolidated using scripts developed in Javascript and Python. To secure the evidence, a decentralized network was designed and implemented using HyperLedger Fabric (HLF) V2.2. Within the network, a smart contract was instantiated, allowing nodes to perform actions on the ledger. And for interaction with peers, client applications were implemented in Node JS using the HLF SDK.

In this experimental phase, positive outcomes were obtained with respect to detection, data size reduction and storage. In this sense, an average reduction up to 60% in the weight of evidence files was achieved. In terms of storage, we were able to maintain immutable records of the transactions carried out. We are currently working on training a model to improve the filtering and dimension reduction. At the same time, we are assessing the mechanisms for incident response and incorporating machine learning algorithms for event correlation.

REFERENCES

[1] "Check Point Software's Mid-Year Security Report. [Online]. Available: https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/."

[2] M. B. Jimenez, D. Fernandez, J. E. Rivadeneira, L. Bellido, and A. Cardenas, "A survey of the main security issues and solutions for the sdn architecture," *IEEE Access*, vol. 9, pp. 122016–122038, 9 2021.

[3] S. Khan, A. Gani, A. W. A. Wahab, A. Abdelaziz, K. Ko, M. K. Khan, and M. Guizani, "Software-defined network forensics: Motivation, potential locations, requirements, and challenges," *IEEE Network*, vol. 30, pp. 6–13, 11 2016.

[4] "The Gartner Board of Directors Survey Reveals 6 Key Statistics. [Online]. Available: https://www.gartner.com/en/articles/6-key-takeaways-from-the-gartner-board-of-directors-survey."

[5] N. M. Karie and C. Valli, "Digital forensic readiness implementation in sdn: Issues and challenges," 7 2021.

[6] E. Salfati and M. Pease, "Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT),"

[7] A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat, and T. R. Gadekallu, "A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions," *IEEE Access*, vol. 10, pp. 11065–11089, 2022.

[8] P. Zinge and M. Chatterjee, "Comprehensive study of digital forensics branches and tools," *The International Journal of Forensic Computer Science*, vol. 13, pp. 22–28, 12 2018.

[9] S. Khan, A. Gani, A. W. A. Wahab, M. Shiraz, and I. Ahmad, "Network forensics: Review, taxonomy, and open challenges," *Journal of Network and Computer Applications*, vol. 66, pp. 214–235, 5 2016.

[10] M. Elyas, A. Ahmad, S. B. Maynard, and A. Lonie, "Digital forensic readiness: Expert perspectives on a theoretical framework," *Computers and Security*, vol. 52, pp. 70–89, 7 2015.

[11] "ISO - ISO/IEC 27042:2015 - Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence [Online]. Available: https://www.iso.org/standard/44406.html."

[12] E. U. A. for Network and I. S. (ENISA), "Electronic evidence -a basic guide for First Responders,"

[13] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer Security Incident Handling Guide Recommendations of the National Institute of Standards and Technology,"

[14] S. hui ZHANG, X. xu MENG, and L. hai WANG, "Sdnforensics: A comprehensive forensics framework for software defined network," pp. 92–99, 12 2016.

[15] H. Munkhondya, A. R. Ikuesan, and H. S. Venter, "A case for a dynamic approach to digital forensic readiness in an sdn platform," *Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020*, pp. 584–593, 2020.

[16] M. Lagrasse, A. Singh, H. Munkhondya, A. Ikuesan, and H. Venter, "Digital forensic readiness framework for software-defined networks using a trigger-based collection mechanism," *Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020*, pp. 296–305, 2020.

[17] M. Pourvahab and G. Ekbatanifard, "An efficient forensics architecture in software-defined networking-iot using blockchain technology," *IEEE Access*, vol. 7, pp. 99573–99588, 2019.

[18] P. T. Duy, H. D. Hoang, D. T. T. Hien, N. B. Khanh, and V. H. Pham, "SDNLog-Foren: Ensuring the integrity and tamper resistance of log files for SDN forensics using blockchain," pp. 416–421, Institute of Electrical and Electronics Engineers Inc., 12 2019.

[19] H. Wang, G. Yang, P. Chinprutthiwong, L. Xu, Y. Zhang, and G. Gu, "Towards fine-grained network security forensics and diagnosis in the SDN era," vol. 14, pp. 3–16, Association for Computing Machinery, 10 2018.

[20] S. A. Mugitama, N. D. W. Cahyani, and P. Sukamo, "An Evidence-Based Technical Process for OpenFlow-Based SDN Forensics," Institute of Electrical and Electronics Engineers Inc., 6 2020.

[21] M. K. Pandya, S. Homayoun, and A. Dehghantanha, "Forensics investigation of openflow-based sdn platforms," *Advances in Information Security*, vol. 70, pp. 281–296, 2018.

[22] M. Pourvahab and G. Ekbatanifard, "Digital Forensics Architecture for Evidence Collection and Provenance Preservation in IaaS Cloud Environment Using SDN and Blockchain Technology," *IEEE Access*, vol. 7, pp. 153349–153364, 2019.

[23] Y. Khan and S. Verma, "An intelligent blockchain and software-defined networking-based evidence collection architecture for cloud environment," *Scientific Programming*, vol. 2021, 2021.

[24] D. Walton and C. Reed, "Evaluating corroborative evidence," *Argumentation*, vol. 22, pp. 531–553, 11 2008.

[25] B. E. Ujcich, S. Jero, A. Edmundson, Q. Wang, R. Skowyra, J. Landry, A. Bates, W. H. Sanders, C. Nita-Rotaru, and H. Okhravi, "Cross-app poisoning in software-defined networking," pp. 648–663, Association for Computing Machinery, 10 2018.

[26] S. B. Kotsiantis, D. Kanellopoulos, and P. E. Pintelas, "Data preprocessing for supervised leaning. world academy of science, engineering and technology," *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, vol. 1, 2007.